

ARTICLE APPEARED
ON PAGE 74BUSINESS WEEK
12 JULY 1982

How 'Bugs' Are Kept Out of the Office

Ten years ago, five "plumbers" broke into Democratic National Headquarters in Washington's Watergate Office Building to replace a defective electronic listening device. They came in the dead of night because they wanted to plant another eavesdropping device disguised as a smoke detector—difficult to do when anyone was around. Today, though, advanced "bugs" are so small that they can casually be salted in an office by a daytime visitor with little risk of detection. Had the White House plumbers squad used such bugs, Richard M. Nixon might have finished his term as President and G. Gordon Liddy might not now be associated with a Niles (Ill.) company that bears his name and specializes in debugging corporate offices.

Counterbugging services are a fast-growing business, trading on the fears of executives and corporate security officers that modern microelectronics technology is being increasingly exploited to steal company secrets. With today's semiconductor technology, tiny radio transmitters with microphones the size of a match head can be hidden in pens, book spines, coat hangers, even picture hooks in a wall. "The trick to bugging is to make it look as if it's not a bug," says Harry A. Augenblick, the president of Microlab/FXR, which makes a bug-spotting

system called SuperScout. Adds Carmine O. Pellosie Jr., vice-president of CCS Communications Control Inc., a New York-based marketer of "hightech" security devices: "Bugging is a very safe thing to do."

Hard to prove. No one knows for sure how much industrial bugging really goes on, but many security consultants—whose opinions are perhaps biased—maintain that it is spreading swiftly. Field agents of the Federal Bureau of Investigation agree to a point, although agent Johnnie Gibson at FBI headquarters cautions that it cannot be proved because no specific data on bugging crimes exist. In a recent survey, corporate security executives overwhelmingly termed bugging a threat, and almost half of them felt that at least 50,000 to 100,000 bugs had been planted in businesses within the last five years.

"Industrial espionage [has been going] up steadily over the years," asserts David L. Watters, an aerospace consulting engineer and former communications researcher at the Central Intelligence Agency. He believes that as much money is spent on industrial espionage as on the combined surveillance efforts of federal, state, and local law enforcement agencies. For industry, Watters figures that the total yearly bill for salaries, equipment, and expenses comes to "hundreds of millions of dollars."

On the other hand, just as many company security officers believe that there has not been any dramatic growth in bugging, despite the advent of ultraminiature transmitters. The perception that it has grown, these officers contend, is the result of better counterespionage measures that are catching more industrial spies. But the claims of corporate security people also may be biased, since an upward trend in industrial espionage could be taken as evidence that they were not doing their jobs.

Souvenirs and cigars. Not surprisingly, no corporate security officer interviewed by BUSINESS WEEK would discuss his own experiences, and many refused to be interviewed. But some of them did relate "sanitized" case histories that have become folklore in the world of corporate security:

"Companies often commemorate special events and successful ventures with plaques or other souvenirs. One entrepreneur figured the mementos could do double duty: In plastic statues given to erstwhile partners who might compete for future business, he secreted a bug. The president of one company grew increasingly suspicious when his competitor kept submitting bids a sliver below his own. One day he emptied his humidor, looking for a bug, but found nothing. Later, he learned that it was in a cigar on the bottom.

"It can be almost impossible to discern individual comments during a crowded meeting because conventional bugs relay monaural signals. So one eavesdropper planted a stereo transmitter in his competitor's boardroom.

Although it is illegal to make, sell, or even possess eavesdropping devices in the U.S., they are not hard to obtain from overseas man-

ufacturers. In West Germany, for example, using hidden listening devices is also forbidden—but making them is perfectly legal. A half-dozen companies sell 12,000 to 14,000 bugs a year, marked "for export only." Frankfurt-based Target Electronics supplies the duty-free shop at the nearby international airport with sophisticated bugging devices that list for as much as \$300. Experts estimate that up to half of all the bugs used by U.S. industrial spies come from abroad.

Even in the U.S., one can legally buy wireless transmitters that are only a bit bigger than real bugs. Radio Shack stores, for instance, carry a model about the size of a small cigarette lighter for \$35. As long as such transmitters are billed as "wireless microphones" or electronic "babysitters," selling and owning one is legal. An accompanying brochure warns against surreptitious use. Even without a ready-made unit, says Pellosie of CCS, "a high school electronics student could build one for \$12," using off-the-shelf parts.

While security experts debate whether the growth of bugging is real or an illusion, no one disputes that the fear of

CONTINUED

Fear of industrial espionage has prompted a booming business in countermeasures

being bugged is soaring—sometimes to the point of paranoia. "Everyone is concerned about the possibility," says the security officer of one multinational corporation. "We have never found a bug," he adds, "but we're sure they're there." "Insurance policy." That sense of insecurity has spawned a booming anti-bug business. Five-year-old CCS notched \$30 million in revenues last year from such equipment as "bionic briefcases" crammed with counterbugging gear. Among the buyers were 50 foreign governments. G. Gordon Liddy Associates, formed 17 months ago by Thomas E. Ferraro, has already branched out to six more cities and expects to collect \$10 million on debugging equipment and consulting fees this year. "Ten years ago hardly anyone was in this business," muses Francis G. Mason, president of F. G. Mason Engineering Inc., a Fairfield (Conn.) antibugging specialist. "Now there are hordes."

Although bug-detection technicians admit that they find evidence of eavesdropping no more than 20% of the time—even 1 bug in 100 sweeps, at \$800 to \$20,000 each, is not uncommon—many companies believe the expense is a necessary prevention. "It's an insurance policy," says the chief security officer at a major bank.

Among the more sophisticated systems is Microlab's \$18,000 SuperScout. It broadcasts a special signal that causes any semiconductor near the "vacuum cleaner" head to resonate; the unit then detects the resonant signal from the chip. Microlab hails the SuperScout, originally developed for the government, as the first sweeper capable of spotting bugs that are not transmitting—even those whose batteries are dead.

Other companies specialize in counterintelligence equipment designed to prevent or deter eavesdropping. Dektor Counterintelligence & Security Inc. in Savannah, Ga., sells a machine that picks up the presence of hidden tape recorders. For about \$300,000, Keene Corp., of Norwalk, Conn., will install electronically shielded walls around a conference room or office. There are "pink noise" or "white noise" machines to mask conversations by showering a room with background noise resembling gently falling rain.

False confidence. Many debugging experts feel that anxious, uncritical executives are often being bilked. Roger Tolces, an industrial security expert in Hollywood, Calif., notes that several security-hardware companies sell a gadget for telephones that is supposed to signal a phone-line tap by lighting up. "But I could bug your phone all day, and your light wouldn't go on," Tolces insists. "Seventy-five percent of the equipment being sold is junk."

Even good equipment may give a false sense of confidence. A determined eavesdropper can break through an electronic room shield simply by drilling a hole in the wall. He could foil the SuperScout by wrapping the bug in aluminum foil or sticking it inside a word processor where its presence would be masked by the machine's own semiconductor chips, notes Joe Wilson Elliott, a former Army intelligence officer who now runs a Los Angeles security company. And the most thorough antibug sweep is negated if someone plants a bug five minutes later.

Still, even jaundiced security experts admit that the new technology has improved their end of the cat-and-mouse game of industrial espionage. "We probably could not have picked up the Watergate bug with 10-year-old technology," says Ferraro of Liddy Associates, whose famous partner was off on the lecture circuit when BUSINESS WEEK called. So what would Ferraro advise the Democrats now? "Sweep their offices every day." The cost? "We'd give them a special deal: only about \$100 a day."

CONTINUED

Lasers get into the eavesdropping act

The most exotic eavesdropping technologies have been developed for the intelligence community, and many of them remain under wraps. But what is known about government surveillance methods offers a chilling glimpse of the future of industrial espionage—if the private sector decides it can afford the equipment.

For example, remote eavesdropping via laser beams eliminates the risk of entering a room to plant bugs; instead, the snooper points a laser at a window and records the otherwise imperceptible vibrations in the glass caused by the sound waves from the conversations inside. But it takes a computer and sophisticated processing equipment to regenerate sound from the window vibrations. "The technology is here," says Carmine O. Pellosie Jr., vice-president of New York-based CCS Communication Control Inc., "but nobody [in industry] spends \$1 million to overhear conversation; they can pick up for \$50."

Clever installation. The bugging schemes that the experts admire are those that ingeniously get around a bug's major limitation: power. The new microbugs may be easy to hide, but their tiny batteries do not last long—a few hours of transmitting time, spread over perhaps two weeks by turning the bug off as much as possible. So top honors go not to the smallest bugs but to those that are cleverly installed to work off their victim's electricity. The classic "para-

site" case: the first bug wired to a light switch, not only eliminating the need for batteries but also saving the eavesdropper from listening to an empty room after the lights were flicked off.

The parasite-bug tactic has since been adapted to other kinds of electrical hardware—the headphones of a secretary's transcription machine, for example. (One counterspy whimsically suggests a black-market trade name for such headsets: Bugman.) Pellosie of CCS cautions his clients: "Beware of any gifts that plug into the wall."

An early precursor of today's laser systems was used by the Russians three decades ago, but probably still would be too expensive for industrial spies. In 1952 the Soviets presented a wooden plaque of the U. S. seal to the U. S. ambassador in Moscow. Flattered, the ambassador hung it on the wall after a thorough inspection revealed no trace of anything remotely resembling a bugging device, but only a hollow metal cavity. The eagle reportedly hung there for six years before U. S. experts figured out its secret: If a microwave radio beam of a certain frequency were aimed at the plaque, the hollow cavity became a resonating chamber that echoed conversations in the room. With special radar-like gear, the Soviets could bounce radio waves off the plaque from a building across the street and listen to the ambassador's conversations.